IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

FOWLER BUICK GMC, INC., individually and on behalf of all similarly situated persons,

Plaintiff,

v.

CDK GLOBAL, LLC

Defendant.

CLASS ACTION COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF

Civil Action No.

CLASS REPRESENTATION

Jury Trial Demanded

Plaintiff Fowler Buick GMC, Inc. ("Fowler" or "Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against CDK Global, LLC ("CDK" or "Defendant"), an Illinois company, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to its own actions, the investigation of their counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for failing to secure its systems and data from cyberattacks, including ransomware attacks. Defendant is a provider of integrated information technology and tools to car dealers and other companies in the automotive industry. Defendant offers solutions that automate and integrate critical workflow processes from pre-sale targeted advertising and marketing campaigns to the sale, financing, insurance, parts supply, and repair and maintenance of vehicles.

2. On or about June 19, 2024, Defendant suffered a ransomware attack, which

prevented Defendant's clients, such as automotive dealers, from conducting their routine and ordinary business, including but not limited to, receiving payment for vehicle and parts sales and vehicle maintenance services provided to the public ("Data Breach").[1]

3. As a result of the Data Breach, and as further described below, Plaintiff was unable to conduct regular business, causing significant business interruption and lost revenues. Additionally, Plaintiff has expended significant time and effort in an attempt to resolve the difficulties and mitigate the financial harms resulting from the breach.

PARTIES

4. Plaintiff is a car dealership located in Pearl, Mississippi. Plaintiff uses software and services provided by Defendant in its daily operations. Plaintiff is a citizen of Mississippi.

5. Defendant CDK Global LLC is a Delaware corporation with its principal place of business headquartered in Hoffman Estates, Illinois. Plaintiff is a citizen of Illinois and this District.

6. Since Defendant shut down following the cyberattack, Plaintiff, among other things, has been unable to obtain payment for the vehicle and parts sales and maintenance services provided to the public. This caused, and continues to cause, Plaintiff to suffer significant monetary losses and other harms.

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed $5,000,000.00,

[1] Christopher Smith, "Dealers Are Set to Lose Nearly $1 Billion over CDK Cyberattack" (Updated July 1, 2024), Motor1.com, https://www.motor1.com/news/725118/dealers-lose-1-billion-cdk-cyberattack/ (last accessed July 2, 2024).

exclusive of interest and costs, and all conditions are met.

8. This Court has jurisdiction over the Defendant as Defendant maintains its corporate headquarters in this District.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in the District and Defendant is headquartered in this District.

GENERAL FACTUAL BACKGROUND

10. Defendant provides integrated information technology and digital marketing solutions to car dealers and other companies in the automotive industry. Defendant offers solutions that automate and integrate critical workflow processes from pre-sale targeted advertising and marketing campaigns to the sale, financing, insurance, parts supply, and repair and maintenance of vehicles.[2] Defendant's primary clients are car dealerships, such as Plaintiff. Defendant serves approximately 15,000 dealerships in North America, which were each affected by the Data Breach. Defendant's software is an "all-encompassing package that handles parts and service work, sales, financing, and payroll." It covers "every aspect" of an automotive dealer's business.[3]

11. According to the *Wall Street Journal*, Defendant's software is essential for all functions inside a dealership—from managing websites to tracking inventory and customer data. Defendant controls nearly 50% of the dealership software market in the U.S., by some estimates.[4]

12. As a condition of receiving its services, Defendant requires its dealer customers to

[2] Bloomberg, "CDK Global LLC", https://www.bloomberg.com/profile/company/1282916D:US?embedded-checkout=true (last accessed July 2, 2024).
[3] Christopher Smith, "Dealers Are Set to Lose Nearly $1 Billion Over CDK Cyberattack" Motor1 (July 1, 2024), https://www.motor1.com/news/725118/dealers-lose-1-billion-cdk-cyberattack/ (last accessed July 2, 2024).
[4] Belle Lin, "CDK Global Hack Shows Risk of One Software Vendor Dominating an Industry" *Wall Street Journal* (June 29, 2024), https://www.wsj.com/articles/cdk-global-hack-shows-risk-of-one-software-vendor-dominating-an-industry-5156420d (July 2, 2024)

entrust them with highly sensitive information, including dealers' customers' personally identifiable information ("PII.")

RANSOMWARE THREATENS THE BUSINESS SECTOR

13. Ransomware is a subset of malware in which the data on a victim's computer, or network, is locked, typically by encryption, and where payment is demanded as a condition of providing the decryption key to unlock the encrypted data and once again make that data available to the victim.[5] The motive for ransomware attacks is nearly always monetary, and the demanded payment is almost always in some form of crypto-currency, typically Bitcoin.[6]

14. Various forms of ransomware have been used to attack corporate as well as individual user systems since as early as 2013. The Cryptolocker strain of ransomware posed as a Trojan horse (malware contained or incorporated within otherwise legitimate-seeming websites, applications, or attachments to emails or messages). In 2017, the WannaCry ransomware attacked and encrypted more than 300,000 Microsoft Windows systems globally, demanding payment in Bitcoin in exchange for the data decryption key. WannaCry's mode of operation closely follows ransomware's general methodology:

> When executed, the WannaCry malware first checks the "kill switch" domain name; if it is not found, then the ransomware encrypts the computer's data, then attempts to exploit the SMB vulnerability to spread out to random computers on the Internet, and "laterally" to computers on the same network. As with other modern ransomware, the payload displays a message informing the user that files have been encrypted, and demands a payment of around $300 in bitcoin within three days, or $600 within seven days.[7]

[5] Ransomware, http://searchsecurity.techtarget.com/definition/ransomware (last visited March 2, 2024)
[6] *Id.*
[7] WannaCry Ransomware Attack, https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (last visited March 2, 2024)

15. While the extortionist's payment demand is relatively small (ranging between hundreds of dollars to tens of thousands of dollars), the damage wreaked on enterprise and other users' systems reaches hundreds of millions of dollars and more.

16. Unlike a data breach, whose seriousness results from the exfiltration and criminal usage of personally identifiable information or personal health care information, a ransomware attack renders data stored within a computer network or individual computer both unreadable and completely inaccessible to the enterprise or computer user. In the case of a health care products or services provider, the consequences can mean life or death.

17. Accordingly, companies hold a large amount of customer PII, such as the Defendant, are especially attractive targets for ransomware. One example of this is Hollywood Presbyterian Medical Center in Los Angeles, who in early 2016 was the victim of a ransomware attack and opted to pay $17,000 in Bitcoin to retrieve the key to unlock its data.[8]

18. Large goods and services providers are not immune from ransomware attacks. In mid-2017, pharmaceutical giant Merck was the subject of the ransomware strain known as "NotPetya." Merck's business was brought to a virtual halt, and the cost to Merck, as of October 2017, amounted to more than $300 million, including more than $175 million in lost business,[9] with the costs to insurers having been estimated at $275 million.[10]

19. Companies that have near-monopolist power, and whose shut-down risks paralyzing an entire industry are even more vulnerable to ransomware attacks. The Data Breach

[8] Richard Winton, Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating, The LA Times (Feb. 18, 2016), http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html (last visited March 18, 2024)

[9] Patrick Howell O'Neill, NotPetya Ransomware Cost Merck More than $310 Million, Cyber Scoop (Oct. 27, 2017), https://www.cyberscoop.com/notpetya-ransomware-cost-merck-310-million/ (last visited March 18, 2024).

[10] Reuters Staff, Merck Cyber Attack May Cost Insurers $275 Million: Verisk's PCS, Reuters (Oct. 19, 2017), https://www.reuters.com/article/us-merck-co-cyber-insurance/merck-cyber-attack-may-cost-insurers-275-million-verisks-pcs-idUSKBN1CO2NP (last visited March 18, 2024).

at issue in this case "shows risk of one software vendor dominating an industry" CDK's dominant position as a service provider to U.S. car dealerships made the entire industry "vulnerable to a 'single point of failure.'" In the words of a prominent technology analyst, "If I was a cyber criminal, of course I would go after CDK. They're the biggest."[11]

20. The ransomware attack should not have come as a surprise to CDK given its market position. It was widely known that ransomware attacks were a threat to large businesses, particularly businesses with a dominant market position, in 2024.

THE RANSOMWARE EVENT AT CDK

30. According to a CDK client note, hackers who gained access to CDK's computer systems made its dealer management system, or DMS, unavailable to its broker clients for days, and were demanding a ransom to restore its systems.[12]

31. As a result of the ransomware attack, CDK shut down the majority of its network, which made it "all but impossible [for dealers] to sell vehicles."[13] In light of the hack, many dealers have started processing transactions manually,[14] significantly slowing down their business processes and decimating their revenues.

32. According to media reports, the BlackSuit cybercriminal gang perpetrated the attack on CDK. BlackSuit is a "relatively new" cybercriminal gang which spun off an older and "well known Russia-linked hacking group" called RoyalLocker. It has breached at least 95

[11] Belle Lin, "CDK Global Hack Shows Risk of One Software Vendor Dominating an Industry" *Wall Street Journal* (June 29, 2024), https://www.wsj.com/articles/cdk-global-hack-shows-risk-of-one-software-vendor-dominating-an-industry-5156420d (July 2, 2024).
[12] Megan Cerullo, "CDK Global calls cyberattack that crippled its software platform a 'ransom event'" (June 25, 2024), https://www.cbsnews.com/news/cdk-attack-cyber-ransom-event/ (last visited July 2, 2024).
[13] Megan Cerullo, "CDK Global cyberattack leaves thousands of car dealers spinning their wheels" CBS News (June 24, 2024), https://www.cbsnews.com/news/cdk-cyber-attack-outage-update-2024/ (last accessed July 2, 2024).
[14] Reuters "Explainer: The 'BlackSuit' hacker behind the CDK Global attack hitting US car dealers" (June 27, 2024) https://www.reuters.com/technology/cybersecurity/blacksuit-hacker-behind-cdk-global-attack-hitting-us-car-dealers-2024-06-27/ (last accessed July 2, 2024).

organizations globally, although the real number of BlackSuit victims is likely much higher, as not all ransomware events are reported publicly.[15]

33. In short, because Defendant's central and mission-critical role in the U.S. healthcare system, a significant proportion of U.S. car dealerships are unable to receive payment for goods and services provided to their clients. This disruption, which started on or about June 19, and the associated financial and other harms, continue to this day. According to analyst Anderson Economic Group, if the outage persists for three weeks, total dealership losses could top $940 million. The analyst notes that this estimate is conservative, does not include "many other categories" of losses, and assumes that new-car buyers stymied by cyberattack will ultimately go though with their planned purchase.[16]

34. What makes the BlackSuit attack so pernicious is that by encrypting (and hobbling) key components of CDK's network, it also hobbled Defendant's, and its dealer clients', ability to conduct their business, effectively shutting down U.S. car dealer industry in its entirety.

PLAINTIFF AND THE CLASS SUFFERED DAMAGES

25. Plaintiff and the Class are CDK's clients, who were unable to conduct normal business due to the Data Breach at CDK.

26. In their everyday practice, and as an integral part of their business, Plaintiff and the Class place significant reliance on their ability to access CDK's systems and transact with CDK.

27. As a direct and proximate result of Defendant's wrongful acts and omissions, Plaintiffs and the Class suffered, and continue to suffer, economic damage and other actual harm,

[15] *Id*.
[16] Christopher Smith, "Dealers Are Set to Lose Nearly $1 Billion Over CDK Cyberattack", Motor1 (July 1, 2024), https://www.motor1.com/news/725118/dealers-lose-1-billion-cdk-cyberattack/ (last accessed July 2, 2024)

including monetary losses arising from significant business interruption and disruption, together with expenses incurred in attempts to mitigate such business interruption and disruption.

28. As of the date of the filing of this Complaint, Plaintiff, and the Class continue to experience significant business interruption and disruption as a direct and proximate result of their inability to conduct normal business operations while Defendant's systems are offline due to the Data Breach.

29. Defendant failed to implement appropriate processes that could have prevented or minimized the effects of the ransomware attack.

30. Plaintiff acted in reasonable reliance on Defendant's misrepresentations and omissions regarding the security of its products and services, and would not have purchased Defendant's products and/or services had they known that Defendant did not take all necessary precautions to protect itself from cyberattack, including ransomware attacks. Plaintiff and the Class would not have gone through with a purchase had they known that the use of Defendant's products was accompanied by an unreasonable risk of business disruption, interruption and monetary loss.

CLASS ACTION ALLEGATIONS

31. Plaintiff seeks relief in their individual capacity and as representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2), (b)(3), and (c)(4), Plaintiff seek certification of the following class:

> All customers of CDK Global, LLC located in the United States who were affected by an interruption of service due to the ransomware attack which occurred on or about June 19, 2024 (the "Class").

32. Excluded from the above Class are: Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by the

Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

33. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, Defendant provides service to 15,000 dealerships in North America, which were each affected by the Data Breach.[17]

34. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant failed to implement, monitor and audit adequate processes to timely detect, prevent, or mitigate a cyberattack;

b. Whether Defendant's failures and omissions constitute a breach of contract;

c. Whether Defendant's failures and omissions constitute negligence, or negligence *per se*;

d. Which security procedures and which data-breach notification procedures should Defendant be required to implement as part of any injunctive relief ordered by the Court;

e. Whether Defendant's acts and/or omissions in respect of the data-breach they suffered on or about June 19, 2024, caused financial harm to the Class Members;

[17] Christopher Smith, "Dealers Are Set to Lose Nearly $1 Billion Over CDK Cyberattack" Motor1 (July 1, 2024), https://www.motor1.com/news/725118/dealers-lose-1-billion-cdk-cyberattack/ (last accessed July 2, 2024).

f. What the nature of the relief should be, including damages and/or equitable relief, to which Plaintiff and Class Members are entitled.

35. All members of the proposed Class are readily ascertainable. Defendant has access to the addresses and other contact information for members of the Nationwide Class, which can be used for providing notice to many Class Members .

36. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because Plaintiff was denied the ability to operate their business, just like other Class Members.

37. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation.

38. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

39. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Nationwide Class.

40. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Defendant has acted or has refused to act on grounds generally applicable to the Class,

so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

COUNT I – NEGLIGENCE AND NEGLIGENCE *PER SE*

(On Behalf of Plaintiff and the Class)

41. Plaintiff repeats and fully incorporates all factual allegations contained in paragraphs 1 through 40 as if fully set forth herein.

42. Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care to safeguard its systems and data from cyberattack, including ransomware attacks.

43. Defendant breached its duties by failing to implement, monitor, and audit the security of its data and systems, resulting in a ransomware attack that significantly impeded and/or prevented its clients' ability to conduct business.

44. Neither Plaintiff nor the Class contributed to the Data Breach as described in this Complaint.

45. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class suffered damages including, but not limited to, disruption and interruption of its business and everyday provision of services to their clients.

46. Defendant's acts and omissions as alleged herein were willful, wanton, and with reckless disregard for the rights of Plaintiff and the Class.

47. As a result of Defendant's negligence, and negligence *per se*, Plaintiff and the Class suffered damages, including costs incurred as a result of business interruption and disruption, together with other damages as may be shown at trial.

COUNT II – BREACH OF CONTRACT

(On Behalf of Plaintiff and the Class)

48. Plaintiff incorporates the factual allegations contained in paragraphs 1 through 40 as if fully set forth herein.

49. Defendant entered into contracts with Plaintiff and Class Members. The contracts state, among others:

> 5. B. ***CDK maintains reasonable security measures designed to: (i) prevent unauthorized access to, or loss or alteration of, Client Data***; and (ii) protect Client Data consistent with applicable state and federal laws, but in no event does CDK guarantee against any unauthorized access, loss or alteration of Client Data. Unless otherwise noted in an addendum hereto or the Product Guide, ***CDK agrees to use commercially reasonable data backup procedures to create backups of Client Data as a part of its data backup and data safeguard procedures***.
> If any Client Data is lost or damaged, ***CDK will use commercially reasonable efforts to restore the most recent copy of such Client Data***; provided, however that CDK cannot guarantee that it will be able to restore or recover any such Client Data.
>
> C. CDK will maintain Client Data relating to a particular Product or Service for the period set forth in the Product Guide (but with the option to extend such retention period for additional fees as and to the extent set forth in the Product Guide), after which Client Data shall be deleted or otherwise destroyed automatically; provided, however, that regardless of any such period(s) set forth in the Product Guide, ***CDK will delete or otherwise destroy all Client Data relating to such Product or Service as soon as practical (and in any event no later than 12 months) following any termination or expiration of the term for such Product or Service***. (Emphasis added).

50. Defendant agreed to provide its specialized services in a professional and workmanlike manner. Implicit in performing these contractual duties is an obligation to reasonably safeguard its systems and data from cyberattack, including ransomware attacks, which can cause an interruption in the flow of an enterprise's routine and everyday provision of services to its clients.

51. Defendant breached its contracts with Plaintiff and Class Members by failing to reasonably safeguard its systems and data from cyberattack, including ransomware attacks.

52. As a direct and proximate result of Defendant's contract breaches, Plaintiff and Class Members sustained actual losses and damages including, but not limited to, complete interruption and disruption of their ability to conduct the regular business of a car dealership.

COUNT III – UNJUST ENRICHMENT

(On behalf of Plaintiff and the Class)

53. Plaintiff repeats and incorporates the allegations contained in paragraphs 1 through 40 as if fully set forth herein.

54. Plaintiff and the Class conferred a benefit on Defendant when they provided payment to Defendant for the sale of its products and services.

55. In exchange for, and in consideration of, Plaintiff and Class members providing payment for Defendant's products and services, Defendant was required to, and Plaintiff and the Class expected Defendant to, implement reasonable security policies and procedures that would have detected, prevented, or mitigated the Data Breach.

56. As a result of Defendant's acts and omissions as alleged herein, Defendant has been unjustly enriched to the extent that any portion of such payments comprises spending for adequate security not provided.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully requests that the Court enter judgment in its favor and against Defendant as follows:

a. For an Order certifying the Class as defined herein, and appointing Plaintiff as class representative;

b. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to ransomware protection;

c. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

d. For an award of actual damages and compensatory damages, in an amount to be determined;

e. For an award of pre-judgment and post-judgment interest as allowed by law;

f. For an award of costs of suit and attorneys' fees, as allowable by law; and

g. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

DATED: July 3, 2024

Respectfully submitted,

/s/ *Shannon M. McNulty*

Robert A. Clifford
Shannon M. McNulty
CLIFFORD LAW OFFICES, P.C
120 North LaSalle Street
36th Floor
Chicago, IL 60602
Telephone: 312-899-9090
rclifford@cliffordlaw.com
smm@cliffordlaw.com

John A. Yanchunis
jyanchunis@ForThePeople.com
Ronald Podolny*
ronald.podolny@forthepeople.com

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

Gerald M. Abdalla, Jr.*
ABDALLA LAW, PLLC
602 Steed Road, Suite 200
Ridgeland, MS 39157
Telephone: (601) 278-6055
jerry@abdalla-law.com

Timothy W. Porter*
PORTER & MALOUF, P.A.
Post Office Box 12768
Jackson, MS 39236
Telephone: (601) 957-1173
tim@portermalouf.com

**pro hac vice to be filed*

Attorneys for Plaintiff and the Proposed Class